Testimony of

Patrick D. Gallagher

Director

National Institute of Standards and Technology

U.S. Department of Commerce

before the

Committee on Small Business and

Entrepreneurship

U.S. Senate

”The Role of Small Businesses in Strengthening

Cybersecurity Efforts in the United States”

July 25, 2011

Introduction

Senator Cardin, members of the Committee, I am Patrick Gallagher, Director of the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce. Thank you for this opportunity to testify today on our perspective regarding the "The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States." We recognize that small businesses play an important role in the U.S. economy. Since use of the Internet is critical in the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber environment cannot be overstated. Today I will focus my testimony on the role small businesses are playing in helping the U.S. Government strengthen our cybersecurity efforts and programs, as well as providing information on NIST's cybersecurity programs and activities that can assist small businesses.

Ensuring that business related information is secure is essential to the functioning of our economy -- and indeed to our democracy. Small businesses, like all organizations, want to embrace and have available the latest advances in technology to make their tasks easier, improve productivity, and remain competitive. But they face an enormous challenge in protecting their information in a cyber environment. In fact, it was recently reported[1] that data and identity theft are impacting small and medium-sized businesses more than individuals.

More than 99 percent of all U.S. businesses are small or medium-sized2; a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security. Many of these businesses house very sensitive personal information, including healthcare or financial information. Many small businesses also provide services to our federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which we all operate, it is vital that this important sector of our economy be aware of the risks and take appropriate steps to ensure their systems are secure. As described in the Department of Commerce's Internet Policy Task Force's paper, *Cybersecurity, Innovation and the Internet Economy*, the rapid development and implementation of sector-specific, consensus-based codes of conduct is critical to protecting the Internet and information innovation sector (I3S) from cybersecurity threats. Through the leadership of NIST and other bureaus, the Department of Commerce can play an important role to convene the I3S and related sectors and industries and facilitate their development of voluntary codes of conduct. Where sectors (such as those with a large number of small businesses) lack the capacity to establish their own voluntary codes of conduct, new and existing NIST guidelines would be available to bridge gaps in security protection.

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. Indeed, the risks to our systems are so complex and pervasive, that we cannot reasonably expect small businesses

[1] "Cybercrime Losses Among SMBs Reach New Highs In Study," http://www.darkreading.com/smb-security/167901073/security/privacy/229402972/cybercrime-losses-among-smbs-reach-new-highs-in-study.html.

[2] "How important are small businesses to the U.S. economy?," http://www.sba.gov/advocacy/7495/8420

to be experts in all areas of security, including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology. It is critical that small business needs and requirements are considered as cybersecurity standards and guidelines are developed.

NIST's mission in cybersecurity is to work with federal agencies, industry, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services. Consistent with this mission and with the recommendations of the President's *Cyberspace Policy Review*, NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach activities. Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users – from small and medium enterprises to large private and public organizations including agencies of the federal government.

NIST's Current Statutory Responsibilities under FISMA

The Federal Information Security Management Act (FISMA), Section 303, states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

While targeted primarily toward federal agencies, the FISMA security standards and guidelines also are used widely by other organizations, including small businesses to help ensure that the information systems supporting enterprise operations are well protected, thereby enhancing competitiveness and productivity.

A sample of some NIST guidance which is available to small businesses is listed below:

- Small Business Information Security: The Fundamentals;
- Guide for Securing Microsoft Windows XP Systems;
- Wireless Network Security;
- Security Considerations for Voice Over IP Systems;
- Guidelines on Electronic Mail Security;
- Guidelines on Securing Public Web Servers;
- Guidelines on Firewalls and Firewall Policy;
- Procedures for Handling Security Patches;
- Contingency Planning Guide for Information Technology Systems;
- Guidelines on Cell Phone and PDA Security;
- Risk Management Guide for Information Technology Systems.

All of these documents, as well as our ITL Bulletins, are available on our web-based Computer Security Resource Center (CSRC) (http://csrc.nist.gov) which provides a wide range of security materials and information to all. CSRC now has over 20 million "hits" annually. The CSRC site also contains many policies, procedures, and practices from both federal agencies and the private sector that are also advertised to the public through NIST's publications and outreach efforts.

We have developed guidance for organizations, large and small, to maximize the security of their information systems so that they may securely conduct business transactions over the Internet. Hardware and software purchased by small businesses today are frequently installed with the original configurations delivered by the vendor, which can often lead to vulnerabilities or other security weaknesses. We are helping small businesses to understand security features and the importance of correct configuration. Even if they have taken steps to minimize the opportunity for inappropriate access by investing in firewall technology and virus protection software, they need to ensure that these technologies are correctly installed, managed, and updated regularly. NIST also created a video that explores the reasons small businesses need to secure their data: http://www.youtube.com/watch?v=ajwX-7jVLo0&feature=player_embedded
Given the state of software insecurity today, vendors frequently issue security patches for their products. Through our outreach efforts, we are advising users of the importance of these patches and where to get up-to-date information and procedures for installing patches.

Interagency Collaborations
In 2002, NIST partnered with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. The workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems. Since May 2010, we have held 24 workshops in 22 cities with 1105 small business owners and employees attending. To expand our outreach efforts, NIST has also developed a Small Business Outreach Site (http://csrc.nist.gov/securebiz/) for easy access to security resources and to provide small businesses with the ability to request a workshop to be held in a specific local area.

For the last four years NIST, in cooperation with SBA and the Association for Small Business Development Centers, has participated in the annual conference of Small Business Development Centers, providing participants with information to increase awareness of NIST resources. NIST is also working with the National Cyber Security Alliance (NCSA) to help make cybersecurity a priority for small businesses (http://www.staysafeonline.org/for-business).

National Initiative for Cybersecurity Education
The National Initiative for Cybersecurity Education (NICE) represents the evolution of the cybersecurity education component of the Comprehensive National Cybersecurity

Initiative (CNCI), expanding it from a federal focus to a larger national focus. NICE was created to meet the cybersecurity training, education, and awareness priorities expressed in Chapter II, Building Capacity for a Digital Nation, of the President's Cyberspace Policy Review[3]. It will enhance the overall cybersecurity posture of the U.S. by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all. The effort is for all U.S. citizens of all ages (pre-school to senior citizens), and all types of professions whether it be in academia (pre-school, K-12, college/universities), federal/state/local government, business (small-medium to large size businesses/companies), or local community group or non-profit organization. The Strategic Plan for NICE will be available for public review and comment in late summer of 2011.

Security Automation

Through the development and adoption of data standards and specifications, security automation harmonizes the vast amount of Information Technology (IT) data into coherent, comparable information streams that inform timely and active management of diverse IT systems. Through the creation of internationally recognized, flexible, and open standards, security automation results in IT infrastructure interoperability, broad acceptance and adoption, improved situational awareness, and creates opportunities for innovation. Security automation standards currently support several initiatives, including widely used configuration checklists and the National Vulnerability Database. These standardized data sources provide a level playing field for security tool developers with innovative ideas, regardless of company size. Commercial off-the-shelf security automation tools also support cost-effective security management for small businesses that lack full-time IT security staff.

IT Product Security Configuration Checklists

IT products are often intended for a wide variety of audiences, so restrictive security configuration controls are usually not enabled by default. As a result, many out-of-the-box IT products are immediately vulnerable. In addition, identifying a reasonable set of security settings that achieve balanced risk management is a complicated, arduous, and time-consuming task, even for experienced system administrators. In order to alleviate some of the burden on all users, and in response to the Cyber Security Research and Development Act of 2002, NIST is facilitating the development and sharing of checklists that indicate settings and optional selections that minimize the security risks associated with computer hardware or software systems. NIST is providing a formal framework for checklist developers to submit checklists to NIST and publishing the checklists for easy access (http://checklists.nist.gov). There are currently more than 175 checklists posted on the website, including, but not limited to, checklists for Internet Explorer 7.0, Internet Explorer 8.0, Microsoft Office 2007, Red Hat Enterprise Linux, Windows 7, Windows Vista, and Windows XP. The checklists, when combined with high-quality guidance and training, substantially reduce the vulnerability of IT systems to attack.

[3] May 29, 2009, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

National Vulnerability Database
The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data. Through NVD, NIST is providing relevant and important information in the area of vulnerability management. Currently the NVD contains information on nearly 47,000 vulnerability advisories with an average of 10 new vulnerabilities added daily. The NVD is relied upon by security tool vendors and end users in both the public and private sectors and is used by the Payment Card Industry Digital Security Standard to help identify key areas of risk within payment card systems.

Software Quality
Small and medium-sized businesses, indeed all organizations, rely on the software used on their information systems. NIST continues to work with industry to improve the security and reliability of software in a variety of domains. For example, we develop standards and test suites for interoperable, robust, quality web applications and products. Our test suites are being used throughout the industry to improve the quality of implementations and specifications. We develop ways to measure the effectiveness of software assurance tools, and conduct research to assess current methods and tools in order to identify problems that ultimately lead to software product failures and vulnerabilities. We conduct research and development in new areas to improve the quality of software, including software trustworthiness. We work with health-related organizations to advance the deployment of electronic health records and to facilitate the development and implementation of a nationwide health information network by developing robust software testing strategies.

National Strategy for Trusted Identities in Cyberspace
As with others, it is critical to small businesses that online services are provided in a secure, trustworthy manner. The recently released "National Strategy for Trusted Identities in Cyberspace[4]," lays out the vision for individuals and organizations, large and small, to be able to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. The Strategy calls for a National Program Office to facilitate the carrying out of the Strategy and the development of interoperable technology standards and policies — an "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The goals of the Strategy are to promote private sector capabilities for protecting individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas in a privacy enhancing manner.

The National Program Office (NPO), to be established within the Department of Commerce, will coordinate the federal activities – including coordination of cooperative public/private efforts - needed to implement NSTIC. The office will be led by NIST with activities involving public policy development and privacy protections to be led by the National

[4] April 15, 2011, *The* ***National Strategy for Trusted Identities in Cyberspace,*** http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Telecommunications and Information Administration. The NPO will have full access to NIST technical expertise, both in the development and acceptance of broad consensus-based standards. NIST has been actively involved in the development and interoperability of secure identity management for many years and recently initiated research into how to make such identity schemes easy to use and hard to misuse.

Cloud Computing

The NIST Cloud Computing program is working with U.S. federal, state and local governments, industry, academia, standards development organizations, and the international community to help identify and develop standards that are needed to keep an open and level playing field for organizations of all sizes in this emerging technology field. NIST is also working to identify and help develop the guidance and technology needed to help organizations and individuals who use cloud computing services to do so securely and effectively. Finally, NIST, through its collaborative initiative to build a US Government (USG) Cloud Computing Technology Roadmap, is helping identify and develop the standards, guidance, and technology that USG agencies need to further adopt the cloud computing model to support their missions more cost effectively, securely, and with improved services. This helps small business on several levels -- directly by helping agencies improve services for small businesses, and indirectly by helping the US government to do its part in encouraging the development of the economically powerful cloud computing model.

The growing development and adoption of the Cloud Computing model supports small businesses on several fronts. It offers an opportunity for small businesses in all sectors to make use of powerful computing resources without requiring an upfront or long-term IT investment in equipment, software, or specialized IT people resources. Small businesses can contract and use computing services through the cloud computing model on a trial basis and only pay for the computing resources they choose to and actually consume. The model is also providing a path for small businesses and others to be able to easily move data and systems from one cloud provider to another.

The emerging Cloud Computing model also offers opportunities for IT sector firms of all sizes by providing cost effective infrastructure and application development platforms, making it easier for innovators and start up firms to enter the IT industry.

Security Focused Research

NIST's near-term effort in Internet security research is directed at working with industry and other government agencies to improve the interoperability, scalability, and performance of new Internet security systems, to expedite the development of Internet infrastructure protection technologies, and to protect the core infrastructure of the Internet.

Looking further into the future, we see the potential for new computational models, such as quantum computing, to threaten the mathematical underpinnings of today's cryptographic systems. In response, NIST is conducting research in the use of quantum information theory to devise network security technologies that do not depend on today's cryptographic techniques. NIST is a key player in the research and development of

biometric standards and systems. We are working with industry and other government agencies to improve the accuracy of biometric systems that utilize fingerprints, face, iris and multi-modal technologies.

With a highly mobile workforce, use of mobile devices is quickly becoming a necessity for small and large organizations. NIST is working in collaboration with industry to improve authentication and encryption techniques associated with these products to ensure that the user's data and wireless communications are protected.

Meeting the challenge of securing our Nation's IT infrastructure demands a greater emphasis on the development of security-related metrics, models, datasets, and testbeds so that new products and best practices can be evaluated. The President's FY 2012 Budget will support NIST's collaborations with industry and academia to develop the necessary metrics and measurement techniques that will be combined to provide an assessment of overall system vulnerability. Utilizing approaches that have been successful in characterizing effects in the physical systems, NIST will develop the necessary measurement science and technologies to secure the Nation's IT Infrastructure.

Small Business support of NIST Cybersecurity Programs

The sharing of cybersecurity standards and practices is more than just a one-way information flow from NIST to the small business community. Through our contracting and acquisition programs, NIST actively engages small business. Important examples of the contributions of small businesses include research, standards support, and products. Small businesses play an important role in NIST's identity and access management research and standards development activities and in determining usability factors that broaden the applicability and improve the effectiveness of security technologies. Small business is a key engine for innovation in the field of cybersecurity. Small business provides critical technical competencies in cutting-edge IT security tools, techniques and test capabilities that permit NIST to leverage their expertise in integrating cybersecurity standards and safeguards into some of our Nation's most critical initiatives, including the development of a secure and interoperable Smart Grid, the adoption of Health Information Technology, and the advancement of automated security vulnerability, asset, and configuration management. As small businesses expand their expertise into new sectors through their relationship with NIST, new opportunities for growth are created.

In addition, NIST relies on small businesses to directly and indirectly support its operational cybersecurity program. Directly, NIST relies on small business contractor labor to assist with the protection of NIST systems and assist with the formal cybersecurity assessment and authorization of NIST systems as required by OMB A-130 and FISMA. Directly and indirectly, NIST relies on small businesses to provide IT support services, such as help desk, out-of-hours system monitoring, desktop and server support, and application development which all play a critical role in protecting NIST computers, networks and information. NIST has also worked closely with small businesses that provide externally hosted applications and services used to support NIST's mission, assessing their security controls against FISMA requirements and

making recommendations on how to improve or implement specific controls to best protect sensitive NIST information processed by their applications and services.

Conclusion

In summary, Mr. Chairman, the IT security challenge facing small businesses is greater than it ever has been. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power. Certainly, there is great potential for malicious activity against non-secured or poorly secured systems or for accidental unauthorized disclosure of sensitive information or breach of privacy.

NIST will continue to develop ways to assist small businesses in their efforts to maximize capabilities and efficiencies offered by emerging technology while minimizing risk to their systems and information. We will continue our work in the areas of trusted identities, secure configuration settings, product benchmarks, outreach, training, and research. The President's FY 2012 Budget will enhance these efforts.

We believe the programs and activities described today demonstrate our commitment to a more effective national cyber security environment by assisting small enterprises in protecting their assets and staying competitive in a cyber economy.

Thank you, Mr. Chairman for the opportunity to present NIST's views regarding security challenges facing small enterprises. I will be pleased to answer any questions that you and the other members of the Committee may have.

Patrick D. Gallagher

Dr. Patrick Gallagher was confirmed as the 14th Director of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) on Nov. 5, 2009. He also serves as Under Secretary of Commerce for Standards and Technology, a new position created in the America COMPETES Reauthorization Act of 2010, signed by President Obama on Jan. 4, 2011.

Gallagher provides high-level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's FY 2011 resources include $750.1 million from the Department of Defense and Full-Year Continuing Appropriations Act, 2011 (Public Law 112-10), $48.6 million in service fees, and $135.6 million from other agencies. The agency employs about 2,900 scientists, engineers, technicians, support staff, and administrative personnel at two main locations in Gaithersburg, Md., and Boulder, Colo.

Gallagher had served as Deputy Director since 2008. Prior to that, he served for four years as Director of the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus. The NCNR provides a broad range of neutron diffraction and spectroscopy capability with thermal and cold neutron beams and is presently the nation's most used facility of this type. Gallagher received his Ph.D. in Physics at the University of Pittsburgh in 1991. His research interests include neutron and X-ray instrumentation and studies of soft condensed matter systems such as liquids, polymers, and gels. In 2000, Gallagher was a NIST agency representative at the National Science and Technology Council (NSTC). He has been active in the area of U.S. policy for scientific user facilities and was chair of the Interagency Working Group on neutron and light source facilities under the Office of Science and Technology Policy. Currently, he serves as co-chair of the Standards Subcommittee under the White House National Science and Technology Council.